107

Posted by u/anon8596541278546 15 hours ago

Open letter to Protonmail about some percieved shifting in policy as it pertains to Not tracking users, Not logging IP address, and being fully anonymous

I checked Archive.is and Internet Archive for previous versions of your website/service and it confirms what I remembered all along, that during the IndieGoGo campaign in which Protonmail successfully gained in close to half a million dollars of donations/ crowd funded investor monies etc the promise (or at least the public pitch) was always that it was "FULLY Anonymous" and that there was "No tracking or logging of personally identifiable information." and again wording of : " No tracking or logging of user data." and also that of "Unlike competing services, we do not save any tracking information. We do not record metadata such as the IP addresses used to log into accounts. We also have no way to scan encrypted messages to serve targeted advertisements. To protect user privacy, ProtonMail does not require any personally identifiable information to register." etc etc etc

https://archive.is/5f1Ja http://archive.is/k8Fhf http://archive.is/yNg5O
https://web.archive.org/web/20140422155106/https://protonmail.ch/

My question is when did this policy change, when did you start tracking IP addressess and logging info and what was the reason and rationale for such a dramatic departure from what you earlier claimed had "set you apart" essentially from the competing services like Google and Yahoo? It is one thing when policies change, but something else when you change something as fundamental to their core essence and value proposition of your service as flip flopping from no-tracking, fully-anonymous, to "yes we are tracking", "yes we proactively cooperate with law enforcement in turning over logging and tracking data" etc; If like the case of the child kidnapping was important enough for you to cooperate with law enforcement of a foreign government without first officially obtaining a valid court order then it should likewise also be important enough for you to be abundantly clear with your end-users and userbase that you do make exceptions to the things that you had essentially earlier promised that you would not infringe upon.

My couple thoughts on this, in the shifting spectrum and wide continium of individual privacy/security (personal privacy rights) vs collective privacy/security (society as a whole as represented by Government in the form of the so-called greater good of the massess) there is always a balancing test or balancing act of sorts. Organizations are never scale-invariant. Smaller companies and projects like Tutanota, Startmail, Countermail etc can "afford" to more or less stay true to their original intent and initial mission statement but whereas larger more "mainstream" services (Protonmail is orders of magnitude larger than all of the other aforementioned combined) has to trade-off some of the more perfect "ideals" (ie such as like saying when "we do not log/track" really means "we don't track/log at all", and not some convoluted situation with Protonmail today where they still claim they don't track but for all intents and purposes they are indeed and infact tracking, etc)

When you look at the security arena folks like David Kahn (author of The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet) and Bruce Schneier when they first had to "break in" to the field and "make a name for themselves" they were all for the individual privacy and individual security rights, they were taking the perspective of an outsider looking in to the abyss/machine, but once they got successful enough they pivoted towards "insider looking out", and essentially Schneier and others have long since abandoned the philosophy of personal or individual privacy/security/rights in favor of collective (government/state) security and that of the "collective greater good of the whole" etc. Google itself for example

COMMUNITY DETAILS

r/ProtonMail

12.0k Subscribers
115 Online

Official subreddit for ProtonMail, an end-to-end encrypted Gmail alternative based in Switzerland.

SUBSCRIBE

CREATE POST

started as a "do no evil" company and for a long time during its nascent years was considered by many as a campaign against Microsoft's bad ways, but as we've seen Google has now far surpassed Microsoft in terms of privacy violations and have become the very thing it intended to avoid. This reminds of the qoute from Batman movie that says : "You Either Die A Hero, Or You Live Long Enough To See Yourself Become The Villain"....

Altough this is an imperfect analogy, but imho Lavabit "died a hero" and if Protonmail continues down this trajectory of the slippery slope and of increasingly becoming "friendlier" and "friendlier" towards all governments and law enforcements alike, having cozzy working relationships with agents, handing out data before the official court order papers even come in, making exceptions so abundantly they become like holes in swiss cheese, and even seemingly insinuating only criminals would be against IP logging/tracking and doing a reverse 180 degree aboutface roundabout with regards to the earlier established policy of "no tracking, no logging, fully anonymous, etc" then it appears Protonmail may turn out -- for better or for worse -- to be "Live Long Enough To See Yourself Become The Villain"

Hey I get it that in order to grow to the size that you guys want to grow to and complete with the likes of Gmail/ Google etc you kinda have to soften your earlier stance in order to gain acceptence in the larger world community and be adopted as a quasi-"controlled opposition" of the governments of the world, where they see it as better to have Protonmail that "cooperates enough" with us than to have a dozen smaller independent services that don't give us visibility and are harder to pressure or persuade etc... And Protonmail taking the stance that its threat model isn't for "snowden" types anyway and is only meant to curb some "mass surveillance" in massee, then bending over backwards in order to be accepted or tolerated by Governments worldwide so in order to continue its massive growth really isn't all that bad of a thing strategically anyway.

My point of contention is that your userbase is getting the rug-pulled-from-underneath-their-collective-feets and it doesn't appear you still have their best interest at heart anymore. In any case, it certainly doesn't seem to be sliding in the right direction. I see Protonmail as a valueable service and I would just like to remind and caution the developers and the company to be aware of these things and be cognizant of the slippery slope, the frog that slowly boils to death, and in essence to be on guard to not bend so much that you wake up one day to find that you've become the very thing you had initially set out to deter against.

I believe that ultimately the market speaks for itself, if you lose sight of the principles that you started out with, and privacy is still important to many, then people will migrate to those services. If you become the next Google and users don't jump ship and still adopt and embrance the "new" Proton/mail, then perhaps in this digital age privacy truly is dead afterall..

==========

Response to Protonmail's well crafted feedback:

Formalities matter to the extent that they are/were used as a selling or pitching point of your product or service. If you had previously stated that Protonmail doesn't cooperate without first obtaining a valid court order, but then go on to make exceptions, then you are going against your own official policy. Again, formalities like this do matter, for example even though courts generally never like to give convicted criminals a free pass nor let anyone guilty off the hook, in a lot of higher court cases and even Supreme Court cases the convictions often do get overtuned/ reversed/ vacated because of a technicality or whenever they rule on an intrepretation. I don't recall exactly which post, but on reddit recently Protonmail took the stance that Protonmail is actually better

than a judge when it comes down to deciding if data should be handed over or something to that effect. Even if assuming that was the case (which I don't necessarily agree with) if you stop following the legal process and due process, stop waiting for the official court order and instead become your own quasi-judge then what else is there left to safeguard? If you directly talk to trusted "agents" and don't wait for the court order itself, then what is the point? At least in the US the FISA court, though it is a rubber stamp, is still followed in terms of process and procedure. But Protonmail should not take place of the judiciary least you give yourself powers that you don't legally have. You stated that it comes down to be about "trust", but we see so many governments and conglomerates alike (including Google) use the often trite "just trust us" excuse. History has shown that is ripe to be taken advantage of. There are technicial safeguards, and there are legal safeguards. The much promised and long overdue ability to import users own pgp keys (technicial safeguard) is no where to be seen and now it appears the legal safeguards (official court order and nothing less will do) is losing its integrity as well...

This matter potentially is further complicated by the fact that you are promoting other services like VPN in the form of ProtonVPN in addition and conjunction to your email service. The common response to those who don't want their IP address tracked when accessing their email is just to use a VPN. But the concern is for a company that went back and regened on its policy of not tracking/logging email users ("fully anonymous") the precedent has already been set for this to happen again and there is no guarantee the same or similiar won't be effectuated for ProtonVPN as well. Imagine a naive user who realized that now that Protonmail is tracking IP and logging access and potentially handing it over to law enforcement or governments that he can protect himself by using a VPN, so he uses ProtonVPN, not realizing that the left hand is (or can be) talking to the right hand.... At the very least, this puts Protonmail in the uncomfortable position of having to make a difficult decision in such edge cases where had the user not consolidated all his privacy services into one Proton, and used for example NordVPN when accessing Protonmail as opposed to ProtonVPN when accessing Protonmail, then this wouldn't have even been an issue in the first place. So we are talking about avoiding single points of failure, both technically (when you get DDoS often both Protonmail and ProtonVPN are down or otherwise inaccessible) as well as from a legal or political standpoint (ProtonVPN may choose in the future to start logging IP addresses or handing them over too, which would entirely defeat the point and purpose of using a VPN (in this case ProtonVPN) in order to prevent tracking/logging from Protonmail)

AFAIK Protonmail's recent aggregation of statistics in the reports of requests was done in the name of being more efficient and expedient. imho, I think the point that is often missed is that the whole point is it is/was intended to make it difficult and not to make it easy. By changing the policy or at least the way request are being reported and by aggregating them in mass that is one step towards trivializing these requests as just another consequence of doing business and very ironically this is the exact very same justification those in power use for the deployment and implementation and usage of "Mass surveillance" in general, which if I'm not incorrect, is the whole point of your service is to counter that.

I realize Proton has a business incentive to attract and intice users to as many different Proton products and services as possible (Protonmail, ProtonVPN, ProtonCoin, etc) but as Proton continues to gain users and grow larger as a company and continue to add more and more new services this only serves to compound the complications and existential dilemmas that one must be confronted with.

But legal process exists for a reason, policy exists for a reason, following it to the letter is important, because outside of technicial controls, if you really think about it, that's all we have left, that's all anybody ever has in truth. The rule of law exists for that reason, and it is nuetral and blind to sides, as it should be. Protonmail should not elevate itself to the position of being the judiciary and making decisions that are required by a judge via a court order.

I would call on Protonmail to think about possibly adopting a "warrant canary" (https://spideroak.com/canary) in the form of the one spideroak has established and a new "bill of rights" for end users to prevent and deter against continuing to slide down the slippery slope. (example : https://spideroak.com/bill-of-rights/)

I encourage protonmail to stay true to the spirit and intent and the letter of its original mission and to do whatever is feasibly possible in the extent that it can so that in order to perpetuate and advance in that front of perserving and protecting individual privacy and unalienable rights.

22 Comments **Share** ••• 85% Upvoted

What are your thoughts? Log in or Sign up LOG IN SIGN UP

SORT BY **BEST**

chdo 27 points · 14 hours ago

i think that they said they updated their privacy policy for clarification after GDRP but that their policies remain the same as always.

and while well-intentioned, you're also a bit underinformed about what's possible when using a centralized SaaS platform. all of the more "ideal" providers you cite would have the ability to log IPs if legally required. Proton's privacy policy actually IS much more clear than competitors in that they're up front about the impossibility of absolute anonymity and quite clear about what information they collect and under what circumstances.

Share **Save**

ProtonMail **ProtonMail Team** 78 points · 13 hours ago 1 · *edited 13 hours ago*

This is the correct answer. Nothing actually changed in our software or our infrastructure, but we decided to switch to more accurate language when GDPR came into effect. Not because the law forced us to do so, but because it is the right thing to do.

Here's the harsh reality. Each time you connect to ProtonMail, your device is sending us your IP address. Yea, that's right, every single request is sending your IP, in real time. And there is no way to get around that. That's just how the internet works. That's how the Internet worked back in 2014 when ProtonMail started, and that's how it works today, and probably also forever into the future.

If asked by Swiss law enforcement to monitor IPs, we may have to do it. It has never happened before because Swiss law enforcement tends to be rather pro-privacy, but it is in theory possible for us to get this request, although it is also in theory possible for us to challenge such a request and stand a reasonable chance of winning. We won't know until we actually get such a request.

This by the way, is a quirk of Switzerland. If you look at the Transparency Reports of the other providers you mentioned (if they have one), you will probably find some surveillance or logging requests. Despite our size, we have never gotten one because it is hard to get a Swiss court to agree to it.

While it definitely IS possible to write a privacy policy that dances around IP processing, we have elected not to do so, and make it explicitly clear that IP logging IS possible.

Now that we have cleared that up, here is what we do to protect your privacy and right to anonymity.

1. When it is practical to do so, we anonymize IP data. It is one thing to have a log of all IP addresses that have connected to ProtonMail and monitor it for abuse. It is another thing to have a list of IPs that have accessed a specific user account. We store and use IP data in the former way, and not later way. But remember, if asked to obtain the later, we have the technical capability to do so, and cannot not have this capability.
2. We delete the IP data that we have regularly. After IP data has been processed

for anti-spam, anti-abuse, or anti-fraud purposes and is no longer needed, we delete it permanently.

3. We provide ProtonVPN, a free VPN service that does not log traffic at all (although again keep in mind, all VPNs can log if they wanted to or if requested by law enforcement, there's no way around this for technical reasons).
4. We also provide an onion address for accessing our site (protonirockerxow.onion) so you can do it directly through the Tor network

Why does Proton use IP data?

We use IP data to keep you safe. The internet is a dangerous place. Many ProtonMail users have sensitive needs, and face serious risks. IP data allows us to identify and monitor botnets and other advanced attackers who are trying to hack into the accounts of ProtonMail users. It also allows us to identify and track attacks carried out against our own infrastructure, helping to keep ProtonMail more secure. Lastly, it also serves as an effective tool to fight spammers. Not fighting spammers effectively would lead to ProtonMail being banned by services around the internet.

Final Thoughts:

Each time you connect to a website, you are going through an Internet Service Provider (if you are using a VPN, the VPN is your ISP). The ISP can always log your traffic, whether or not they actually do it or not, is something you have to trust them on. So there is a reasonably good possibility that your ProtonMail activity is also being logged by your ISP.

Therefore, if anonymity is really your thing, then protonirockerxow.onion is for you, and that's precisely why we have invested significant resources into maintaining an onion site and being perhaps the only Tor encrypted email: https://protonmail.com/tor

This is something none of the other providers you mentioned above have done, and it is the only way to achieve anonymity. Others may claim anonymity without going through an onion site, but that is not an entirely truthful claim given how the internet works, and you will not find us making that claim.

Share **Save**

naQVU7IrUFUe6a53 29 points · 13 hours ago

I love how u/protonmail spells it out completely for the angry trolls on the internet. Thank you for providing such a great service!

Share **Save**

ProtonMail **ProtonMail Team** 34 points · 13 hours ago

Just to comment on a few other assertions from OP:

> handing out data before the official court order papers even come in

We're now in the 21st century. Waiting for registered mail is not a productive exercise, so once we get a digital request, that is sufficient. We have not had a single incident where after getting a digital request we didn't get the formal request in the mail.

> becoming "friendlier" and "friendlier" towards all governments and law enforcements alike, having cozzy working relationships with agents

This is also not really correct. We only have a relationship with a single government, and that is the Swiss government via the Swiss Federal Police and the Swiss Justice Department. As we discussed previously, a close relationship is an asset, as it ensures the officers we work with do a good job of vetting requests before they become enforceable.

https://www.reddit.com/r/ProtonMail/comments/8v1xap/protonmail_policy_in_edge_cases_of_giving_away/e1k2x75/

Share **Save**

termapt **Windows | Android** 2 points · 4 hours ago

> While it definitely IS possible to write a privacy policy that dances around IP processing, we have elected not to do so, and make it explicitly clear that IP logging IS possible.

I guess the problem that causes posts like the OP's is that you kind of did write a

policy that danced around IP logging. Before the changes, the policy explicitly stated that you only logged IPs when enabled by the user, when in fact you logged them from the beginning regardless of user decision.

I don't think that change is that big of a deal, but the whole situation could've been avoided if you'd made the policy clear from the beginning.

Share **Save**

drakonka 2 points · 3 hours ago

This is what I was thinking as I read through the response. Suddenly now they decided to make their policy "more clear" with the GDPR coming into effect (but totally not because of the GDPR guys, just out of the goodness of their hearts because it's "the right thing to do"), so it turns out before they were keeping their policy purposefully vague? Where was the sense of righteousness before GDPR came in?

Share **Save**

damn_dede 2 points · 11 hours ago

it makes sense because Switzerland is often a neutral country who wishes to support business instead of State imposed regulations... a good choice!

Share **Save**

anon8596541278546 -7 points · 12 hours ago (3 children)

Rafficer **Windows | Linux | Android** 9 points · 13 hours ago

Another thing that gets left out is that (if I'm not mistaken, I would be happy to be confirmed or denied by ProtonMail) the IPs are logged in HTTP logs that are not connected to an individuals Account.

This is also necessary to find bruteforce attacks. If a single IP tries 300 times a minute to log in, it's most likely not a human and that IP can be blocked temporarily. To come to that conclusion you don't need the Account they try to log into, you just need a timestamp and an IP Address.

Share **Save**

Soulflare3 2 points · 12 hours ago · *edited 11 hours ago*

Here is an example of Apache's access.log from one of my servers. You can see an attempted brute-force attack on phpmyadmin's login page. This should give an idea of just some of the information that could be collected by a server, and this is just default Apache.

Note: phpmyadmin wasn't used for anything anyway (I haven't used MySQL in years), but has also been disabled.

Quick summary:

- IP
- Date
- Time
- Timezone offset
- Request Type
- File/directory requested with query string
- Protocol
- Status codes
- Bytes transferred
- Useragent (Browser, OS, Architecture, etc.)

apache documentation

Share **Save**

GolferRama 7 points · 11 hours ago

Bottom line is there are only so many email privacy options on the internet today. Protonmail, Tutanota, and a few others.

Protonmail is by far the easiest to sign up with a free account and just get going. That's why it's used and loved by so many.

Having said that we should be diligent and ask questions but the response from Protonmail on reddit and other spaces on the internet has been nothing short of incredible.

I will be a paying Protonmail.com customer for a long time. Can't thank them enough and when the calendar comes I'll be ditching all other email providers.

Share **Save**

8bitMotherFucker 6 points · 9 hours ago

Ultimately, it's a judgment call about who you trust more: ProtonMail vs the alternatives. I trust PM to respect my privacy more than their competitors. If the day comes that they give me a reason to feel differently, e.g. they start freely giving up data on customers when there's no justifiable reason to, then I'll bounce and spend my money elsewhere.

They still are subject to, and must comply with, the law. They can reject orders that aren't valid, they can challenge orders that are valid but overreaching or dangerous, but they aren't here to protect criminals. If they outright refused to comply with the law, PM would already be a sinking ship.

Share **Save**

maggotbrain777 7 points · 8 hours ago

Serious troll is serious.

So many folks have come out of the woodwork in the last year to 'help' ProtonMail in bikeshedding their project.

IMHO I don't think the PM founders entered the email provider market lightly. There will always be room for technical and legal improvement. PM (and Tuanota) has done a pretty solid job provided email services despite the competition.

I realize that I have put my trust in a 3rd party for my communications. Currently, I am OK with that. The effort that ProtonMail has made with the development of their client, bridge, and ESPECIALLY their VPN client, is off to an awesome start. If I had need to be legitimately paranoid, I might consider hosting my own mail server. If OP is serious about their personal security and privacy, they might consider the cost/benefit of relying on a 3rd party for their needs.

This whinging and 'demanding' ProtonMail assuage their fears is pretty silly. Their efforts towards transparency has been commendable.

/half-assed rant off

Share **Save**

ResponsibleDoughnut 2 points · 14 hours ago · *edited 13 hours ago*

I don't speak for Protonmail but the change in logging policy might have something to do with the new surveillance laws passed in 2015.
https://protonmail.com/blog/swiss-surveillance-law/
https://tutanota.com/blog/posts/stop-buepf
https://www.reddit.com/r/privacy/comments/3pm21z/switzerland_to_make_surveillance_of_citizens_easy/

Share **Save**

ProtonMail **ProtonMail Team** 16 points · 13 hours ago

No, this is not correct. ProtonMail is in the class of companies that are specifically exempted from having to comply with that low. This is an exception that we sought and obtained during the process of lobbying against the law (including holding a public referendum on it).

Share **Save**

ResponsibleDoughnut 1 point · 12 hours ago

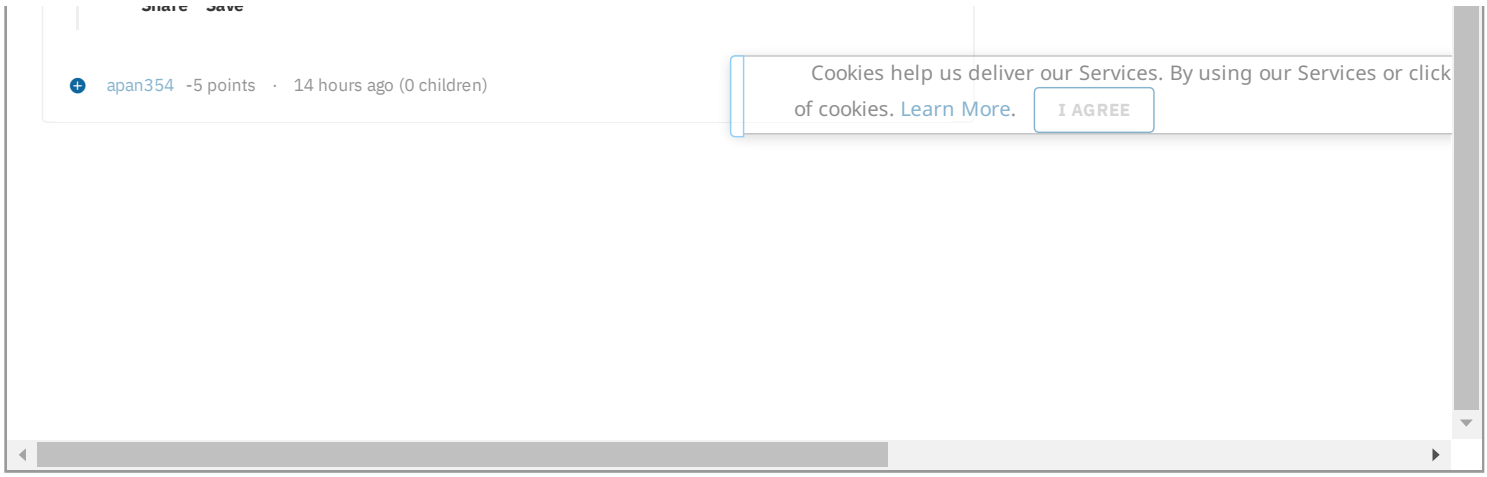
Thanks for clarifying!

Share **Save**

userkp5743608 1 point · 5 hours ago

Wall of text FUD. You're wasting Reddit's server space.

Share **Save**


apan354 -5 points · 14 hours ago (0 children)
Cookies help us deliver our Services. By using our Services or click
of cookies. Learn More.
I AGREE